



**PWYLLGOR ARCHWILIO A SICRWYDD RISG
AUDIT AND RISK ASSURANCE COMMITTEE**

DYDDIAD Y CYFARFOD: DATE OF MEETING:	23 February 2021
TEITL YR ADRODDIAD: TITLE OF REPORT:	Counter Fraud Update
CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:	Huw Thomas, Director of Finance
SWYDDOG ADRODD: REPORTING OFFICER:	Ben Rees, Head of Counter Fraud

Pwrpas yr Adroddiad (dewiswch fel yn addas)

Purpose of the Report (select as appropriate)

Er Gwybodaeth/For Information

**ADRODDIAD SCAA
SBAR REPORT**

Sefyllfa / Situation

This report provides to Audit & Risk Assurance Committee the Counter Fraud update on the work completed within Hywel Dda University Health Board (HDdUHB). This ensures compliance with the Welsh Government (WG) Directives for Countering Fraud in the NHS and the NHS Counter Fraud Authority Standards for NHS Bodies (Wales). The report will present a breakdown as to how resource has been used within Counter Fraud, alongside an overview of key work areas completed against the 4 NHS Counter Fraud Authority generic standard areas.

Cefndir / Background

To evidence the provision of services within a sound governance framework.

Asesiad / Assessment

The Health Board is compliant with the WG Directives.

Argymhelliad / Recommendation

The Audit & Risk Assurance Committee is requested to receive this update for information.

Amcanion: (rhaid cwblhau)

Objectives: (must be completed)

Committee ToR Reference Cyfeirnod Cylch Gorchwyl y Pwyllgor	5.2 In particular, the Committee will review the adequacy of: 5.2.4 the policies and procedures for all work related to fraud and corruption as set out in National Assembly for Wales Directions and as required by the Counter Fraud and Security Management Service.
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol:	Not applicable

Datix Risk Register Reference and Score:	
Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	Governance, Leadership and Accountability
Amcanion Strategol y BIP: UHB Strategic Objectives:	Not Applicable
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Statement	Not Applicable

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	Counter Fraud Workplan 2020/21
Rhestr Termiau: Glossary of Terms:	LCFS – Local Counter Fraud Specialist
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Archwilio a Sicrwydd Risg: Parties / Committees consulted prior to Audit and Risk Assurance Committee:	Not Applicable

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Not Applicable
Ansawdd / Gofal Claf: Quality / Patient Care:	Not Applicable
Gweithlu: Workforce:	Not Applicable
Risg: Risk:	Not Applicable
Cyfreithiol: Legal:	Not Applicable
Enw Da: Reputational:	Not Applicable
Gyfrinachedd: Privacy:	Not Applicable
Cydraddoldeb: Equality:	Not Applicable



HYWEL DDA UNIVERSITY HEALTH BOARD

COUNTER FRAUD UPDATE 2020/21

For Presentation 23rd February 2021

The NHS Protect Standards are set in four generic areas:

- Strategic Governance
- Inform and Involve
- Prevent and Deter
- Hold to Account

AREA OF ACTIVITY	Resource Allocated (days) 2020/21	Resource Used (as at 31/01/2021) (days) 2020/21
STRATEGIC GOVERNANCE	45	31
INFORM AND INVOLVE	90	67.5
PREVENT AND DETER	85	65.5
HOLD TO ACCOUNT	200	111
TOTAL	420	275

Work Area	Summary of work areas completed
Inform and Involve	<ul style="list-style-type: none"> • A total of 383 new staff have completed the Health Board's induction programme since 1st December 2020. • Counter Fraud content on the Health Board's Medicines Safety learning days has again been delivered to nurses by way of virtual sessions. Further sessions are to be arranged throughout the year. • A Fraud Awareness and Risk Management input was delivered to the Finance Department by way of a virtual presentation. • A quarter 4 / winter edition of the Fraud reporter has been published, highlighting some recent cases across the UK along with providing information and guidance reference vaccination scams, the prevalence of which has seen a sharp increase in recent months. A copy is appended to this report for Committee Members' perusal at Appendix 1. • Since the last CF update, a total of 5 Global awareness messages were issued surrounding the following topics: <ul style="list-style-type: none"> - COVID-19 vaccination scams affecting HB and local authority staff. - COVID-19 vaccination scams affecting Primary Care / members of the public. - HB and local scam advice - General Fraud awareness and the publication of the most recent edition of the Fraud Reporter. • In order to engage with a wider audience, the CF Department has engaged with our colleagues in the communications department, Local Authority and CFS Wales to provide awareness on the increase of vaccination scams. • A draft Information Sharing Protocol request is due to be reviewed by the Information Governance Team.
Prevent and Deter	<ul style="list-style-type: none"> • 2 Alerts have been disseminated to relevant stakeholders within the Health Board and Departments within Quarter 4. These included alerts related to DPD Phishing scams and patients at risk of committing fraud against the NHS. • Following a Task and Finish Group meeting concerning the Recovery of Overpayments and Management of

	<p>Underpayments Policy, a Final draft has been reviewed by Workforce and is due to be discussed at the next Partnership Forum (February 2021) before formal sign off by PPPAC.</p> <ul style="list-style-type: none"> • Fraud Risk Assessments have been generated by the CF department and will be discussed with the relevant Service Lead for monitoring and review. • A proactive exercise has been undertaken in connection with Fraud risks associated with the recruitment process. This includes virtual document checking, and employment checks undertaken by both recruitment and employment agencies who provide staff to the HB. A report on this will be presented at the April 2021 ARAC In-Committee session. • A request is made to incorporate Fraud Risk monitoring within future ARAC reports, where the CF department will report on Fraud Risks identified and management responses. The importance of notifying the Counter Fraud Department of any identified fraud risks within directorates will be highlighted in future Fraud Awareness sessions.
Hold to Account	<ul style="list-style-type: none"> • Several new referrals have been received in the past 2 months. These and case updates have been documented in a separate report, for discussion during the In-Committee session.
Strategic Governance	<ul style="list-style-type: none"> • Quarter 3 statistics have been submitted to Counter Fraud Service Wales and in compliance with WG directions.
Other matters	<ul style="list-style-type: none"> • Terry Slater has completed the first and commenced the second module of his LCFS Accreditation Course, which should result in him obtaining accreditation by April 2021. • The National Fraud Initiative (NFI) Data is currently going live, meaning that some work can be undertaken in this area in Q4 and in the new financial year.

Report Provided by:

Ben Rees

Lead Local Counter Fraud Specialist

For presentation; 23rd February 2021

Report agreed by:

Huw Thomas, Director of Finance



THE FRAUD REPORTER

Welcome to the Winter Edition of The Fraud Reporter

Welcome to the Winter edition of the Fraud Reporter, the Hywel Dda UHB newsletter to keep you up-to-date with fraud issues affecting the Health Board and wider NHS.

Once again Covid-19 continues to have an impact on the NHS and our communities. Recently we have seen an increase in the amount of ~Covid-19 Vaccination related scams in the NHS, Local Authority and community settings.

Techniques seen recently have included bogus emails with links claiming to have important updates which, once clicked on, lead to devices being infected. Cyber criminals pose as people they're not, such as staff within government organisations, banks and suppliers. Attacks also take place as phone calls.

Although the National Cyber Security Centre has taken measures to automatically discover and remove malicious sites which push phishing and malware, the current level of attacks will have a more damaging impact since the NHS has less capacity to respond quickly to mitigate the damage.

With the increasing stress on the NHS, especially those at the front line of the fight against Covid-19,

there is an even greater imperative that existing protocols are adhered to. Any attempts to circumvent the normal rules and procedures could leave an organisation wide open to cyber criminals and others to take advantage and have a catastrophic effect.

It is important that everyone is extra vigilant and individual users are aware that SPAM emails and scam phone calls are on the increase.

To avoid systems becoming infected or individuals and organisations compromised colleagues should:

- Be vigilant and suspicious – if something looks too good to be true it generally is. If an email comes from a colleague but doesn't sound like them and isn't formatted in the way they would write – be suspicious. Call your colleague to check.
- Never give out your own or anyone else's passwords, bank details or other sensitive data. A legitimate organisation will
- NEVER ask for this data via email (or telephone). If in any doubt don't say anything and seek advice. It is best to be cautious.
- Check links in any password reset (or other) emails very carefully – check they are taking you to a legitimate site. If in doubt, navigate to the site directly (without using the email link) and log-in directly. This is a common "phishing" technique.
- Don't open attachments from anyone you don't know or that are not from a trusted source.
- Don't reply to spam or forward chain emails.
- Change your passwords regularly and do not use the same password for all accounts, both at home or at work.
- Do not unsubscribe from any unsolicited "spam" emails – this just confirms you are a real address.

Inside this issue:

NHS CFA Fraud Awareness Animations.	1
Vaccination Scams	2
Gang stole £320k from NHS.	2
Cyber Gang target NHS in £1 million pound scam.	3
LCFS Contact Details	4

Fraud Awareness Training

Remote Training Available

One of the key aims of an LCFS is to develop an anti-fraud culture within the Health Board and ensure that staff can spot fraud when it occurs so something can be done about it.

Training can be tailored to the fraud risks for your specific work area and can be delivered at a time and place that suits you and your team.

Contact the LCFS on
01267266268 /
01267266280 or email


Benjamin.Rees2@wales.nhs.uk

Terry.Slater@wales.nhs.uk


To arrange your fraud training.

NHS Counter Fraud Authority Animations

The NHS CFA have a number of animations relating to Fraud in the NHS. If you would like to learn more about fraud in the NHS and the different types of offences seen within the sector please take a few minutes to view one or more of the available animations via the 'What is NHS Fraud' page on our Counter Fraud Service intranet page.




GOV.UK/coronavirus



Counter Fraud Authority

COVID-19: VACCINE FRAUD

Criminals are using the COVID-19 vaccine as a way to target the public by tricking them to hand over cash or financial details. They are sending convincing-looking text messages letting people know they are eligible for the vaccine or phoning people directly pretending to be from the NHS, or local pharmacy.




PEOPLE ARE WARNED TO BE ALERT TO THESE SCAMS:

The **NHS** will:


- ✗ NEVER ask for payment - the vaccine is free
- ✗ NEVER ask for your bank details
- ✗ NEVER arrive unannounced at your home to administer the vaccine
- ✗ NEVER ask you to prove your identity by sending copies of personal documents such as your passport

TOP 4 VACCINE SCAMS




TEXT MESSAGES

People are asked to press a number on their keypad or to send a text message to confirm they wish to receive the vaccine, doing so is likely to result in a charge being applied to their phone bill and fraudsters collecting personal information to use again.




PHONE CALLS

Victims receive a phone call from a fake caller offering the vaccine for a fee or asking for bank details.




WEBSITES

Fake URL links to convincing-looking NHS vaccine booking forms, these look like official NHS forms and may contain some personal information already, at the end of the form it asks for their bank details.




IN PERSON

Fraudsters are calling unannounced at the homes of victims by pretending to be from the NHS to administer the vaccine there and then, in exchange for a cash payment.



GOV.UK/coronavirus



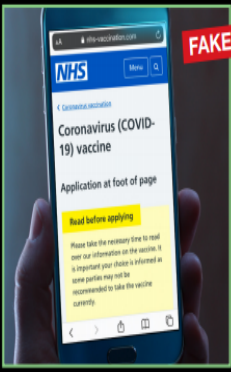
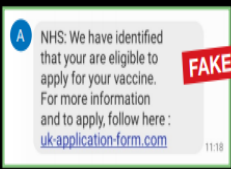
Counter Fraud Authority

COVID-19: VACCINE FRAUD

LIKE OTHER SCAMS, THE SAME ADVICE APPLIES:

- 1 Challenge** - Could it be fake? It's ok to reject, refuse or ignore any requests that don't feel right. Check GOV.UK to ensure it's genuine.
- 2 Do not respond** to text messages that try to get you to send money, or important personal information such as bank details or passwords.
- 3 Use official government websites** and refer to 'Contact Us' sections of websites to access information and service.
- 4 Challenge** unannounced callers to your home, NHS visits if necessary will be agreed with you directly or via carers, they will never turn up unannounced.

EXAMPLES OF SCAMS

A Gang is accused of fleecing Worcestershire's hospitals of more than £322,000

Solomon Adeyemi, Emmanuel Nbangwa and his wife Remilekun Olusesi did not enter pleas to fraud, theft and money laundering against Worcestershire Acute Hospitals NHS Trust when they appeared before magistrates in Worcester yesterday.

The trust runs Worcestershire Royal Hospital in Worcester and the Alexandra Hospital in Redditch.

The case involves the alleged theft of medical equipment and supplies.

The Prosecution said: "Mr Nbangwa was in the employ of the NHS and is alleged to have been stealing theatre equipment from the hospital (the Alexandra) where he worked. As a result of this role he was then organising the procurement to purchase items back from a company established by him."

The case involves the alleged theft of single use supplies from operating theatres which were then said to be sold back to the trust.

The prosecutor told magistrates that the total value of the alleged theft and fraud was £322,482 made up of invoices paid by the trust, the value of invoices received for which no payment was made and the value of stock recovered during a search.

Solomon Adeyemi is accused of entering into/being concerned in the acquisition, retention or use of criminal property by fraudulently obtaining payments from the NHS trust between October 23, 2017 and February

7, 2020.

He faces a charge of concealing/disguising/converting or transferring criminal property by making cheque payments and electronic transfers into the personal accounts of his two co-defendants and the business account of Lawyis Medical UK Ltd between December 27, 2017 and November 7, 2019.

Emmanuel Nbangwa, is charged with fraud by abuse of position while working for the acute trust as a materials management assistant at the Alexandra Hospital in Redditch.

It is alleged that he 'dishonestly abused that position' between October 23, 2017 and September 11, 2019.

The defendant also faces a charge of theft by an employee of £291,833 from the trust between October 23, 2017 and September 11, 2019.

The prosecutor said the loss to the trust had 'huge consequences and financial implications on an already strained public purse'.

The original article published by Worcester News can be found here;

[Gang 'stole £320K from Worcester hospital in huge NHS fraud' | Worcester News](#)



A CYBER gang has tricked the NHS into sending £1million of taxpayers' cash into their bank accounts.

The crooks targeted accounts staff, getting them to substitute their details for those of real suppliers. The cash was diverted into the bogus accounts and moved at high-speed through several others to disguise the trail.

The crime only comes to light when the supplier realises, they have not been paid.

Investigators say they uncovered the "sophisticated mandate fraud" at one NHS body. They have obtained material from 220 bank accounts suspected of being involved and have analysed 107 digital devices including computers, hard drives, laptops and phones.

It has led to 11 people being arrested and a further 16 have been interviewed under caution.

The activity was revealed in the annual accounts of the NHS Counter Fraud Authority.

The body believes the health service is susceptible to £1.2billion a year in bribery, fraud and corruption.



Fears of fraud in the supply chain have been heightened by the [Covid pandemic](#), with the NHS having to act quickly to secure equipment and drugs.

Labour MP Chris Evans said: "Any fraud in the NHS needs to be investigated thoroughly to root out wrongdoing."



Counter Fraud Authority

STOP

Taking a moment to stop and think before parting with your money or information could keep you safe

CHALLENGE

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT

If attempt is noticed in work, contact the Counter Fraud Team or outside work contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.



How to protect yourself:

- Don't assume a call, text or email is genuine.
- Never provide financial or personal details to a caller.
- Don't click on website links or download attachments in unexpected texts or emails.
- Phone numbers and emails can be changed (spoofed) and are not proof of identity.
- Challenge every request for your information, money or details.
- Double check requests for your details and verify via a trusted source.

We can't stop crime we don't know is happening

If you suspect a Fraud has occurred in your area of work then please contact Ben Rees or Terry Slater on the details below



010267 266268 / 01267266280

- Benjamin.Rees2@wales.nhs.uk
- Terry.Slater@wales.nhs.uk

Further, up-to-date information around fraud and scam threats emerging as a result of Covid-19 is available on the Health Board's intranet page.

Further Information

With fraud and cyber crime on the rise across the UK its a good idea that we all know how to deal with scams if we find ourselves unlucky enough to be in that situation. Action Fraud lead the fight against fraud and cyber scams in the UK and they have issued some simple rules to follow to stay safe.

You will find more advice via clicking on the following link

<https://www.actionfraud.police.uk/>

Further advice is available from the Take Five—To Stop Fraud campaign which is a Government backed initiative to reduce fraud <https://takefive-stopfraud.org.uk/about/take-five/>

YOU CAN SEARCH COUNTER FRAUD ON THE HYWEL DDA INTRANET FOR FURTHER INFORMATION

The Health Board's Counter Fraud Team are responsible for raising awareness of fraud, preventing fraud through 'fraud proofing' exercises and investigating fraud where uncovered.

The Counter Fraud Team are always happy to offer advice about NHS fraud, bribery and corruption.

The LCFS is available to support, guide and assist on all fraud, bribery and corruption matters. If you need any advice on fraud or if you want to request counter fraud training for your team please contact your LCFS.

The Counter Fraud Team

Benjamin Rees—Head of Local Counter Fraud Services

☎ 01267 266268

✉ Benjamin.Rees2@wales.nhs.uk

Terry Slater —Local Counter Fraud Specialist

☎ 01267 266280

✉ Terry.Slater@wales.nhs.uk

✉ HDUHB.CounterFraudTeam.HDD@wales.nhs.uk

You can also make a report anonymously you can call the Fraud & Corruption Reporting Line on

0800 028 40 60

or search 'NHS Fraud' online for more information.

STOP NHS FRAUD

www.reportnhsfraud.nhs.uk

0800 028 4060

POWERED BY CRIMESTOPPERS